

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-351747

(43)Date of publication of application : 06.12.2002

(51)Int.Cl. G06F 12/16  
G06F 3/06  
G06F 12/00  
G06F 12/14

(21)Application number : 2001-163202

(71)Applicant : HITACHI LTD

(22)Date of filing : 30.05.2001

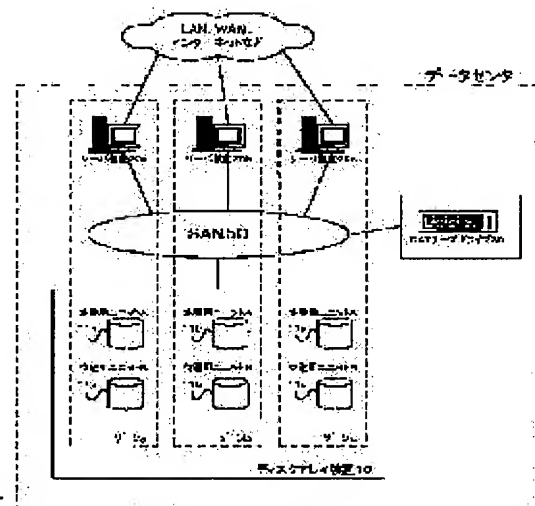
(72)Inventor : SUZUKI HIROYOSHI  
TAJI IWAU

(54) BACKUP MANAGING METHOD FOR IN-STORAGE DATA OF STORAGE SYSTEM AND STORAGE SYSTEM EQUIPPED WITH MEANS FOR IMPLEMENTING THE SAME MANAGING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a backup managing method for in-storage data of a storage system which can assure high data security.

SOLUTION: The storage system includes a storage 10 having a plurality of storage areas 11 given access restrictions individually and a removable media type backup device 30. When the data in a certain storage area 11 are backed up, the data are ciphered with a key given uniquely to the storage area 11 and the ciphered data are stored in specified removable media set in a backup device through SAN 50. When the data in the certain storage area 11 are reloaded, the removable media are set in the backup device, the ciphered data stored in the media are transmitted to the storage 10 through the SAN 50, deciphered with the key given to the storage area 11, and stored into the storage area 11.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-351747

(P2002-351747A)

(43)公開日 平成14年12月6日(2002.12.6)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 12/16	3 1 0	G 0 6 F 12/16	3 1 0 M 5 B 0 1 7
3/06	3 0 4	3/06	3 0 4 F 5 B 0 1 8
12/00	5 3 1	12/00	5 3 1 M 5 B 0 6 5
	5 3 7		5 3 7 H 5 B 0 8 2
12/14	3 2 0	12/14	3 2 0 B

審査請求 未請求 請求項の数5 O L (全 7 頁)

(21)出願番号 特願2001-163202(P2001-163202)

(22)出願日 平成13年5月30日(2001.5.30)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 鈴木 啓悦

神奈川県小田原市中里322番地2号 株式会社日立製作所SANソリューション事業部内

(72)発明者 田路 巖

神奈川県小田原市中里322番地2号 株式会社日立製作所SANソリューション事業部内

(74)代理人 100071283

弁理士 一色 健輔 (外5名)

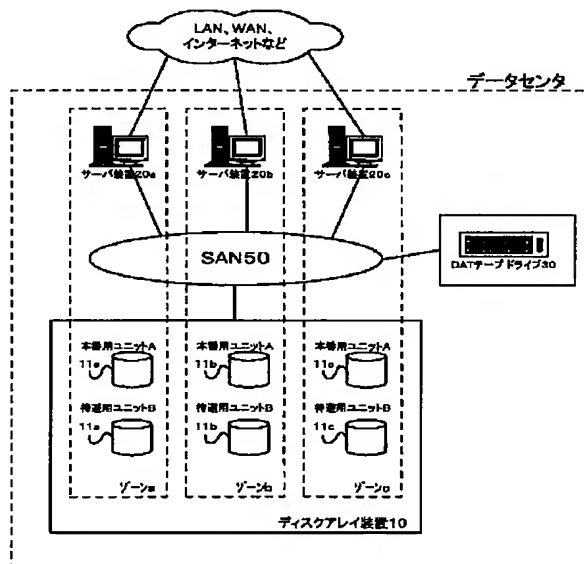
最終頁に続く

(54)【発明の名称】 ストレージシステムにおけるストレージ内データのバックアップ管理方法およびこの管理方法を実施する手段を備えたストレージシステム

(57)【要約】

【課題】 高いデータセキュリティを確保することができる、ストレージシステムにおけるストレージ内データのバックアップ管理方法を提供する。

【解決手段】 個別にアクセス制限が施された複数の記憶エリア11を有するストレージ10とリムーバブルメディア方式のバックアップ装置30を含むストレージシステムにおいて、ある記憶エリア11のデータのバックアップに際してはその記憶エリア11に固有に付与したキーにより暗号化してその暗号化データをバックアップ装置にセットされている所定のリムーバブルメディアにSAN50を通じて格納し、ある記憶エリア11のデータの復旧に際しては該当のリムーバブルメディアをバックアップ装置にセットしてこれに格納されている暗号化データをSAN50を通じてストレージ10に伝送しこれを前記記憶エリア11に付与されたキーにより復号化して前記記憶エリア11に格納する。



## 【特許請求の範囲】

【請求項 1】 個別にアクセス制限が施された複数の記憶エリアを有するストレージとこのストレージにアクセスするサーバ装置とリムーバブルメディア方式のバックアップ装置とが所定の通信手段によりネットワーク接続されているストレージシステムにおけるストレージ内データのバックアップ管理方法であって、

前記記憶エリアのうちのある記憶エリア A のデータのバックアップに際しては記憶エリア A のデータを記憶エリア A に固有に付与したキーにより暗号化した暗号化データを前記通信ネットワークを通じて前記バックアップ装置にセットされている所定のリムーバブルメディアに格納し、

記憶エリア A のデータの復旧に際しては該当のリムーバブルメディアを前記バックアップ装置にセットしてこれに格納されている暗号化データを前記通信ネットワークを通じて前記ストレージに伝送し、これを記憶エリア A に付与された前記キーにより復号化して記憶エリア A に格納することを特徴とする。

【請求項 2】 請求項 1 に記載のストレージシステムにおけるストレージ内データのバックアップ管理方法であって、

前記所定の通信手段が S A N であり、  
前記記憶エリアが一台もしくは複数台のハードディスクユニットにより提供され、

前記ハードディスクユニットのうちのあるハードディスクユニット A のデータをそのハードディスクユニットに固有に付与したキーにより暗号化してこの暗号化データをハードディスクユニット A とは別の前記ハードディスクユニットに記憶管理し、

ハードディスクユニット A のデータのバックアップに際しては前記暗号化データを前記 S A N を通じて前記バックアップ装置にセットされている所定のリムーバブルメディアに格納し、

ハードディスクユニット A のデータの復旧に際しては該当のリムーバブルメディアを前記バックアップ装置にセットしてこれに格納されている暗号化データを前記 S A N を通じて前記ストレージに伝送しこれをハードディスクユニット A に付与された前記キーにより復号化してハードディスクユニット A に格納するようにすることを特徴とする。

【請求項 3】 請求項 2 に記載のストレージシステムにおけるストレージ内データのバックアップ管理方法であって、前記アクセス制限が前記 S A N のゾーニング機能もしくはマスキング機能により設定されたものであることを特徴とする。

【請求項 4】 請求項 2 に記載のストレージシステムにおけるストレージ内データのバックアップ管理方法であって、前記暗号化データを前記ハードディスクユニット A に格納されているデータの変更に応じてリアルタイム

に生成し、前記暗号化データを前記ハードディスクユニット A とは別の前記ハードディスクユニットに同時並行的に記憶管理することを特徴とする。

【請求項 5】 請求項 1 ～ 4 のいずれかに記載のバックアップ管理方法を実施する手段を備えたストレージシステム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、ストレージシステムにおけるストレージ内データのバックアップ管理方法に関し、とくにリムーバブルメディア方式のバックアップ装置を利用してストレージ内データを集中的にバックアップ管理する際におけるデータセキュリティを確保するための技術に関する。

## 【0002】

【従来の技術】 A S P 市場の拡大、企業システムのアウトソーシング指向に伴い、データセンタの需要が増大している。典型的なデータセンタにおけるストレージシステムの概略構成を図 6 に示す。ディスクアレイ装置などのストレージ 10 と、L A N や W A N、インターネットなどを通じてデータセンタ外の機器に接続しこれらとストレージ 10 との間に介在するサーバ装置 20 a、20 b、20 c と、ストレージ 10 内のデータをバックアップするバックアップ装置 30 (D A T テープドライブ) とが S A N (Storage Area Network) 50 により接続されている。

【0003】 ところで、データセンタにおいては、データの一括管理によるスケーラブルメリットを最大限に生かすため、一台のストレージ 10 に異なるシステムや異なるユーザのデータを混在させて運用管理するのが一般的である。そのため、データセンタでは、通常、ストレージ 10 内に実装されたハードディスクユニットなどの各記憶資源について、ゾーニングやマスキングなどの機能を用いてシステムごと或いはユーザコンピュータごとのアクセス制限を施すことで、データセキュリティの確保を図っている。

【0004】 一方、データセンタではディスククラッシュなどのトラブルに対する危機管理も重要であり、通常、データセンタでは S A N 50 の特徴を生かした L A N フリー・バックアップやサーバ・フリー・バックアップといった手法を用いて S A N 50 に接続されたバックアップ装置 30 により集中的なバックアップ管理を行っている。なお、前記のバックアップ装置 30 としては、ビット単価の比較的安価な D A T テープドライブなどのリムーバブルメディア方式のものが採用されることが多く、バックアップ装置 30 にはリムーバブルメディアの脱着を行うためのオペレータが配置されるのが普通である。

## 【0005】

【発明が解決しようとする課題】 ところで、前記のリム

ーバブルメディアの脱着に際しては、オペレータには細心の注意が要求される。何故なら、万が一、指定されたメディアと異なるメディアを間違えてバックアップ装置30にセットしてしまった場合には、あるシステムやユーザ用にアクセス制限された記憶資源に他のシステムやユーザのデータが格納されてしまうこととなり、データセンタの信用にかかわる重大な事故につながるおそれがあるからである。

【0006】しかしながら、オペレータも人間であるからこのような人為的なミスを完全に防ぐことは難しく、従って、このような事故を未然に防ぐ仕組みを設けることがデータセンタの運用上好ましい。

【0007】本発明はこのような観点からなされたものであって、高いデータセキュリティを確保することができる、ストレージシステムにおけるストレージ内データのバックアップ管理方法およびこの管理方法を実施する手段を備えたストレージシステムを提供することを目的とする。

【0008】

【課題を解決するための手段】この目的を達成するための、本発明の主たる発明は、個別にアクセス制限が施された複数の記憶エリアを有するストレージとこのストレージにアクセスするサーバ装置とリムーバブルメディア方式のバックアップ装置とが所定の通信手段によりネットワーク接続されているストレージシステムにおけるストレージ内データのバックアップ管理方法であって、前記記憶エリアのうちのある記憶エリアAのデータのバックアップに際しては記憶エリアAのデータを記憶エリアAに固有に付与したキーにより暗号化した暗号化データを前記通信ネットワークを通じて前記バックアップ装置にセットされている所定のリムーバブルメディアに格納し、記憶エリアAのデータの復旧に際しては該当のリムーバブルメディアを前記バックアップ装置にセットしてこれに格納されている暗号化データを前記通信ネットワークを通じて前記ストレージに伝送し、これを記憶エリアAに付与された前記キーにより復号化して記憶エリアAに格納するようにしたものである。

【0009】

【発明の実施の形態】図1に本発明の一実施例として説明する、データセンタに設置されたストレージシステムの概略構成を示している。ファイバチャネルストレージとして機能するディスクアレイ装置10と、LANやWANもしくはインターネットなどの外部ネットワークを介してこのデータセンタの利用者である企業などのコンピュータに接続しこれらとディスクアレイ装置10との間に介在するサーバ装置20と、DATテープドライブ30とが、ファイバチャネルスイッチやファイバチャネルブリッジなどのネットワークデバイスで構成されたSAN50に接続され、ストレージシステムを構成している。

【0010】図2はディスクアレイ装置10の概略構成である。複数台のハードディスクユニット11が実装され、これら制御するドライブ制御部12、SAN50との間の接続を制御するチャネル制御部13、共用メモリ14やキャッシュメモリ15、ディスクアレイ装置10内の各種制御や稼働状況監視、障害検知および各種情報管理（例えば、実装されているハードディスクユニット11の物理シリンダ数やアクセス頻度などの管理）などを行うサービスプロセッサ16などを備えている。

【0011】ハードディスクユニット11には、ファイバチャネルスイッチおよびディスクアレイ装置などが備えるゾーニングやマスキングなどの機能によってアクセス制限が施されている。例えば、図1の場合では、ハードディスクユニット11a、11b、11cにそれぞれ個別にアクセス制限（ゾーンa、b、c）が施され、ハードディスクユニット11a、11b、11cはそれぞれ独立した記憶エリアを構成しており、例えば、サーバ装置20aはゾーンaのハードディスクユニット11aにはアクセスできるが、ゾーンbのハードディスクユニット11bやゾーンcのハードディスクユニット11cにはアクセスすることはできない。

【0012】ディスクアレイ装置10のハードディスクユニット11の一部は、サーバ装置20aからの直接的な読み出しや書き込みが可能な本番用ユニットAに割り当てられ、また、他の一部は本番用ユニットAのバックアップデータを格納するための待避用ユニットBに割り当てられている。各本番用ユニットAと待避用ユニットBとの対応づけは、システム管理者などがディスクアレイ装置10の管理端末などから手動で設定する方法、サービスプロセッサ16が、例えば、各ハードディスクユニット11が実装されているスロットの位置を自動認識して設定する方法などの各種の方法により設定される。ディスクアレイ装置10は、この本番用ユニットAと待避用ユニットBとの対応付けを、各ハードディスクユニット11に付与された固有のユニットIDにより図3に示す管理テーブルに記憶管理している。

【0013】待避用ユニットBに格納されるバックアップデータは、本番用ユニットAのデータそのものでなく、これを暗号化したものである。ディスクアレイ装置10は、各本番用ユニットAのデータをリアルタイムに暗号化し、各本番用ユニットAに対応づけられている待避用ユニットBにリアルタイムに格納する。これにより待避用ユニットBには、本番用ユニットAのデータの暗号化データが同時並行的に記憶管理される。

【0014】暗号化は、各本番用ユニットAとこれに対応づけられた待避用ユニットBのペアごとに固有に設定されたキーを用いて行われる。キーは、ディスクアレイ装置10により自動的に生成される場合、システム管理者などにより手動で設定される場合など、様々な方法で設定される。キーは、本番用ユニットAと待避用ユニッ

10

20

30

40

50

トBの組み合わせに対応づけて前記管理テーブルに記憶管理される。

【0015】ところで、この実施例で説明するストレージシステムでは、本番用ユニットAのデータのバックアップに際し本番用ユニットAのデータをそのままバックアップするのではなく、これに対応づけられている待避用ユニットBに格納されている暗号化データの方をバックアップするようにしている。これはバックアップに関する一連の処理が本番用ユニットAに与える負荷を極力抑え、本番用ユニットAを利用している各種システムやユーザへの影響を減らすためである。

【0016】バックアップはつぎの手順で行われる。まず、ディスクアレイ装置10は、SAN50を通じてDATテープドライブ30にDATテープのセット指示を送信する。これによりDATテープドライブ30は、付属の管理用ディスプレイにDATテープをセットするよう表示する。ここでこの指示には、バックアップ対象となる本番用ユニットAを特定するユニットIDが含まれ、管理用ディスプレイには前記セット指示に付帯してユニットIDも表示される。オペレータは、これらの表示を確認すると、該当の本番用ユニットA用に用意されたDATテープを管理ラックから探し出してDATテープドライブ30にセットする。

【0017】つぎに、DATテープが正常にセットされると、その旨がSAN50を通じてディスクアレイ装置10に通知され、バックアップ対象となる本番用ユニットAに対応する待避用ユニットBに格納されている暗号化データが、SAN50を通じてディスクアレイ装置10からDATテープドライブ30に伝送されて、前記DATテープに前記暗号化データが格納される。暗号化データのDATテープへの格納が完了すると、管理用ディスプレイにその旨が表示される。これを見たオペレータはDATテープをDATテープドライブ30から取り外し、そのDATテープを管理用ラックの所定位置に収納する。

【0018】一方、DATテープにバックアップされた暗号化データは、例えば、ディスククラッシュなどにより本番用ユニットAのデータが紛失等した場合のデータの復旧処理に利用される。つぎに、この復旧処理の手順を図4に示すフローチャートとともに説明する。

【0019】ディスクアレイ装置10は、ある本番用ユニットAに何らかの異常が発生し、DATテープにバックアップされた暗号化データを利用する必要があると判断すると、DATテープドライブ30にその本番用ユニットAに対応する暗号化データ（すなわち、この本番用ユニットAに対応する待避用ユニットBからバックアップした暗号化データ）が格納されているDATテープのセット指示を、SAN50を通じて送信する（110）。DATテープドライブ30は、このセット指示を受信すると、その旨およびこのセット要求通知に付帯す

る前記本番用ユニットAのユニットIDを、管理用ディスプレイに表示する（120）。オペレータは、このセット指示を確認すると、該当のDATテープを管理ラックから探し出し、そのテープをDATテープドライブにセットする（130）。

【0020】DATテープが正常にセットされると、つぎに、その旨がSAN50を通じてディスクアレイ装置10に通知され、DATテープドライブ30にセットされているDATテープに格納されている暗号化データが、ディスクアレイ装置10に伝送される。ディスクアレイ装置10は、伝送されてきた暗号化データを、前記本番用ユニットAに対応づけられている待避用ユニットBに格納する（140）。

【0021】以上により暗号化データが待避用ユニットBに格納されると、つぎに、ディスクアレイ装置10は管理テーブルを参照し、前記本番用ユニットAに対応づけられているキーにより待避用ユニットBに記憶されている暗号化データの復号化を試みる（150）。ここでこのキーが待避用ユニットBに格納されている暗号化データの暗号化の際に使用したキーと一致する場合には、正常に復号化が行われ、ディスクアレイ装置10は復号化されたデータを前記本番用ユニットAに格納し、これにより前記本番用ユニットAのデータ復旧処理が無事完了する（160）。

【0022】他方、キーが不一致の場合には、復号化を行うことができず、この場合、ディスクアレイ装置10は、当該装置10の管理端末のディスプレイなどにその旨を通知するエラーメッセージを表示する（170）。そして、これを見て復号化ができなかったことを知ったシステム管理者は、DATテープの掛け間違えたかどうかをオペレータに確認し、掛け間違えであった場合には、オペレータに正しいDATテープをDATテープドライブ30にセットし直してもらうなどの対応を講じることとなる。

【0023】以上に説明したように、本発明によれば、万が一、オペレータがDATテープを掛け間違えてセットしても、あるシステムやユーザにアクセスが許可されたハードディスクユニットに他のシステムやユーザの暗号化データが格納されてもキーが一致しない以上その暗号化データが復号化されることはなく、高いデータセキュリティが確保されることになる。また、万が一、DATテープが盗まれても、キーが知られない以上、元のデータを復元することはできず、この点でもデータセキュリティが確保されることになる。

【0024】ところで、以上の実施例は、待避用ユニットBに格納されている暗号化データをバックアップする構成であったが、例えば、本番用ユニットAのデータをディスクアレイ装置10が直接暗号化し、この暗号化データを直接SAN50を通じてDATテープドライブ30に伝送してリムーバブルメディアにバックアップし、

データ復旧時には該当のDATテープに格納されている暗号化データをDATテープドライブからSAN50通じてディスクアレイ装置10に伝送して復号化する、といった構成も考えられる。なお、この方式を採用した場合には、図1に示すように各ゾーンに必ずしも複数のハードディスクユニットが含まれている必要はなく、一つのゾーンに一台のハードディスクユニットしか含まれなくてもよいことになる。

【0025】アクセス制限は必ずしも前述の実施例で説明したようにハードディスクユニット単位に設定する必要はなく、例えば、1台のハードディスクユニットの記憶エリアを分割し、分割された記憶エリアごとに異なるアクセス制限を施す、といったアクセス制限の仕方も考えられる。

【0026】本番用ユニットAと待避用ユニットBとは前述の実施例のように1:1に対応づけられていてもよいし、1:nに対応づけられていてもよい。

【0027】ストレージは、ディスクアレイ装置である場合に限られず、磁気ディスクシステムや光磁気ディスク装置（共に充分な容量のキャッシュやバッファを備えたもの）などでもよい。

【0028】バックアップ装置は、前述したDATテープドライブ以外に、例えば、カセットテープ、8mmテープ、9トラック・オープン・テープ、3490/3490Eカートリッジ・テープ、DLT/SDLTテープ、AITテープ、TRAVANミニカートリッジ・テープ、DTFカートリッジ・テープ、LTOカートリッジ・テープ、ZIP、CD-R、DVD-RAM、DVD-R、MO、フロッピー（登録商標）ディスクなどのメディアを用いるものであってもよい。

【0029】また、一般にストレージに実装されるハードディスクユニット11は、RAIDを構成していることが多いが、本発明はRAIDを構成しているかどうか\*

\*に関わらず適用することができる。

【0030】キーは、前述の実施例のように暗号化と復号化の双方に同一のキーを設定してもよいし、暗号化キーと復号化キーとを別個に設定してもよい。なお、この場合、暗号化キーと復号化キーは、例えば、図5に示すような形態で管理テーブルに管理されることになる。

【0031】また、以上の説明では秘密鍵方式を前提とするものであるが、公開鍵暗号化方式を採用することも考えられる。

【0032】

【発明の効果】以上説明したように、本発明によれば、高いデータセキュリティを確保しつつ、ストレージシステムにおけるストレージ内データのバックアップ管理を行うことが可能である。

【図面の簡単な説明】

【図1】本発明の一実施例による、データセンタに設置されたストレージシステムの概略構成を示す図である。

【図2】本発明の一実施例によるディスクアレイ装置の概略構成を示す図である。

【図3】本発明の一実施例による管理テーブルの一例を示す図である。

【図4】本発明の一実施例による、本番用ユニットのデータの復旧処理を説明するフローチャートである。

【図5】本発明の一実施例による管理テーブルの一例を示す図である。

【図6】従来のデータセンタにおけるストレージシステムの概略構成を示す図である。

【符号の説明】

10 ディスクアレイ装置

11 ハードディスクユニット

20a, 20b, 20c サーバ装置

30 バックアップ装置（DATテープドライブ）

50 SAN

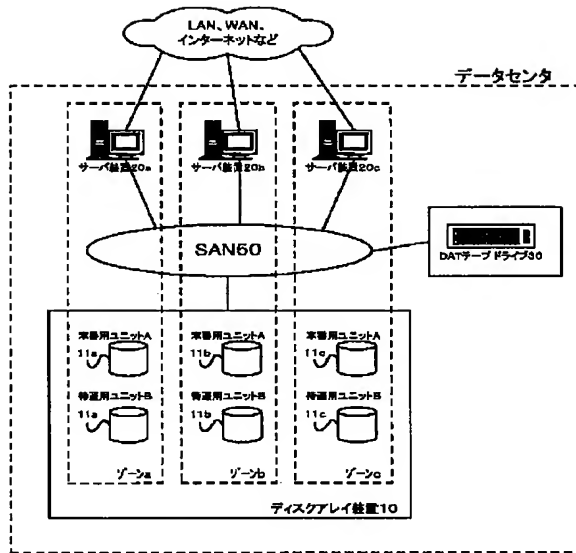
【図3】

本番用ディスク のユニットID	待避用ディスクの ユニットID	暗号化キー
500	600	xxxvyyzzz
114	116	xxxzzzyyy
118	120	wwwsskkk
.	.	.
.	.	.
.	.	.
.	.	.

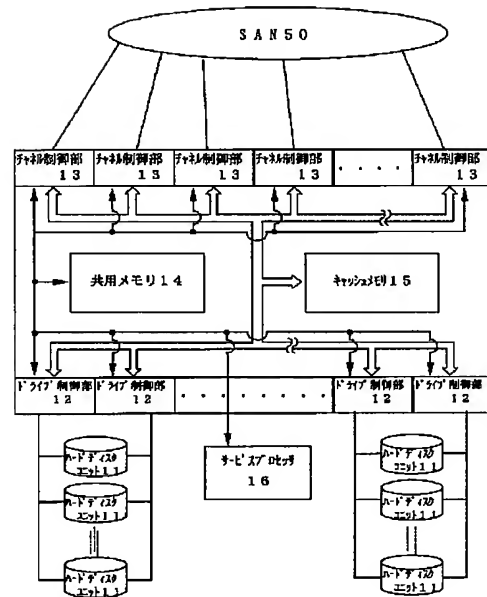
【図5】

本番用ディスク のユニットID	待避用ディスクの ユニットID	暗号化キー	復号化キー
500	600	xxxvyyzzz	ssskddjii
114	116	xxxzzzyyy	pppqqquuu
118	120	wwwsskkk	yyyrrii
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.

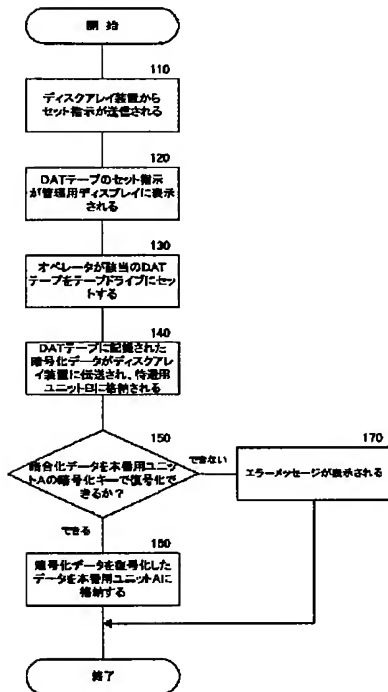
【図1】



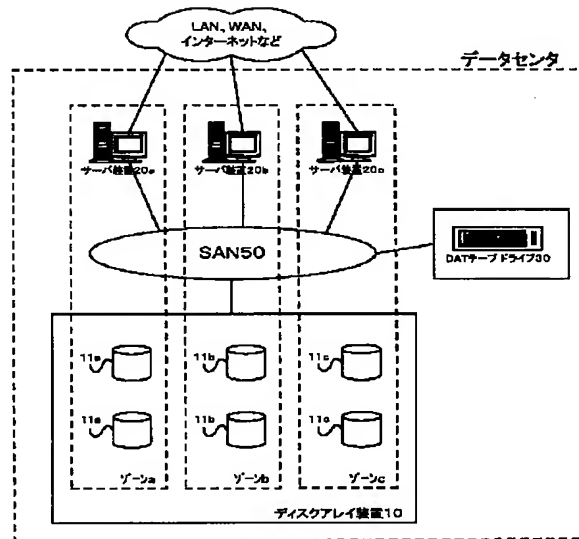
【図2】



【図4】



【図6】



フロントページの続き

Fターム(参考) 5B017 AA03 BA07 CA07  
5B018 GA04 GA10 HA04 KA03 MA12  
5B065 BA01 BA07 CA19 CE22 EA12  
EA35 PA16 ZA15  
5B082 DE04 DE07 GA11 HA05